Web4 Reference Implementation: A Seven-Layer Sovereign Stack by LINKSPREED

Companion Technical Report to the Sovereign-Ownership Architecture Specification

Marc Herdina

LINKSPREED GROUP — Web4 Division

hello@linkspreed.com | web4.one | linkspreed.com

ABSTRACT

Abstract*—This companion technical report specifies the concrete reference implementation of the Web4 seven-layer sovereign-ownership architecture developed and operated by the LINKSPREED GROUP. Where the accompanying architectural specification [1] defines the layers L1–L7 in abstract, standards-composition terms, this report describes the seven named components that instantiate them — UIID (sovereign identity substrate), VIVON (physical mobile access layer), ARCTIC (decentralized compute mesh), HELION (intelligent routing and naming), TRIVE (DID-authenticated service layer), ATRIUM (sovereign application delivery), and WYNIX (certified consumer hardware) — together with the concrete protocol bindings, deployment topology, product surfaces, and operational security posture that instantiate the Ownership Thesis defined in [1]. This report is intended as a companion document to [1]: the architectural claims, the security analysis, and the standards positioning are given in the architecture paper; the concrete component realization is given here. Readers seeking the architectural justification and comparative positioning of the seven-layer stack should consult [1] first.*

Index Terms*—Web4, LINKSPREED, UIID, VIVON, ARCTIC, HELION, TRIVE, ATRIUM, WYNIX, sovereign identity, decentralized compute, sovereign application delivery, reference implementation, DID method, digital sovereignty.*

Companion Statement. *This report is a companion technical report to the architectural specification "Web4: A Seven-Layer Sovereign-Ownership Architecture for the Next Generation of the Internet" [1] by the same author. The architectural claims, formal Ownership Thesis, standards positioning, and security analysis are stated and defended in [1]. The purpose of the present report is to specify the concrete LINKSPREED reference implementation of that architecture — the mapping from abstract layers L1–L7 to named product components — and to document the operational surfaces, protocol bindings, and deployment characteristics of that implementation.*

I. INTRODUCTION AND RELATION TO THE ARCHITECTURAL PAPER

The architectural specification of Web4 published in [1] introduces and defends the Ownership Thesis — the axiom that every layer of the network stack must be reducible to a claim controlled by a decentralized identifier that the subject holds directly — and derives from that axiom a seven-layer reference architecture consisting of a sovereign identity substrate (L1), a sovereign physical access layer (L2), a decentralized compute mesh (L3), an intelligent routing and naming layer (L4), a DID-authenticated service layer (L5), a sovereign application-delivery layer (L6), and a sovereign hardware layer (L7). Together these layers realize the fourth verb of the web — ACT — in addition to READ, WRITE, and OWN, by binding autonomous-agent action to time-boxed, DID-scoped capability grants rather than to developer-scoped static API keys.

The present report is the concrete companion to [1]. Its purpose is not to re-argue the Ownership Thesis or to re-position Web4 against Web1–Web3 or against the competing contemporary definitions of Web4 catalogued in [1, Section II-F]; those arguments are given once, in [1], and are incorporated here by reference. The purpose of this report is to specify the seven named components — UIID, VIVON, ARCTIC, HELION, TRIVE, ATRIUM, and WYNIX — that constitute the LINKSPREED reference implementation of the seven-layer architecture, and to describe the concrete deployment, product surfaces, and operational characteristics of each.

The remainder of this report is organized as follows. Section II summarizes the mapping from abstract layers to named components. Sections III–IX specify each of the seven components in turn. Section X describes the end-to-end request lifecycle in the deployed implementation. Section XI documents the current release status and roadmap. Section XII concludes.

II. MAPPING FROM ABSTRACT LAYERS TO NAMED COMPONENTS

Table I provides the mapping between the abstract layer designations used in the architectural paper [1] and the concrete component names used in the remainder of this report. All architectural properties claimed for a layer in [1] apply to the corresponding named component below.

TABLE I

Abstract Layer → LINKSPREED Reference Component

Layer	Abstract Designation (per [1])	Component Name	Concrete Realization
L1	Sovereign Identity Substrate	**UIID**	Universal Integrated Identity Decoupled; did:uiid method with Core and Alias Identifiers.
L2	Sovereign Physical Access Layer	**VIVON**	Global eSIM connectivity; UIID-native calling and messaging endpoints.
L3	Decentralized Compute Mesh	**ARCTIC**	Agentic-compute mesh, Zk-Storage sharding, ARCTIC OS, BFT consensus.
L4	Intelligent Routing and Naming Layer	**HELION**	Linkspreed Name Service (LNS), W4 OS, OXYGEN browser, W4 Search, Web4 Bridge.
L5	DID-Authenticated Service Layer	**TRIVE**	UIID-authenticated B2B and B2C tool suites over UIID KV storage.
L6	Sovereign Application Delivery Layer	**ATRIUM**	Super Apps as a Service (SNaaS); AI-orchestrated deployment via 1-Prompt AI Method.
L7	Sovereign Hardware Layer	**WYNIX**	W4 Phone as personal server; ARCTIC micro-server for Web4@Home.

III. UIID — SOVEREIGN IDENTITY SUBSTRATE (L1)

A. Component Overview

UIID (Universal Integrated Identity Decoupled) is the LINKSPREED reference implementation of the L1 sovereign identity substrate specified in [1, Section IV-A]. UIID defines the did:uiid DID method: a globally unique, URI-formatted identifier of the form did:uiid:<method-specific-id> which resolves through the Linkspreed Name Service (LNS) at Layer 4 to a DID Document containing verification methods, service endpoints, and controller information, in accordance with W3C DID Core [2], [3].

B. Core and Alias Identifiers

UIID defines a two-tier identity model. The Core Identifier is the immutable, sovereign root of a subject's identity; it is never disclosed directly to third-party services and is used exclusively for first-party operations within the UIID Dashboard, such as authorizing new applications or reviewing audit records. Alias Identifiers are subordinate, context-scoped identifiers — for example a financial alias, a professional alias, or a social alias — issued as Verifiable Credentials that cryptographically reference the Core Identifier without disclosing it to a relying party. Authentication follows a passwordless flow combining WebAuthn with Zero-Knowledge Proofs; access is bounded by granular scopes such as core:write and alias:read:private; mandatory Multi-Factor Authentication protects critical operations; and transparent audit-log endpoints record every issuance and verification event.

C. UIID v2.8 — Multi-Entity Framework and Agent Factory

The UIID v2.8 release of June 2026 extends the substrate from human-only identity to a comprehensive multi-entity framework covering six specialized entity types: Human Individual, Organization, AI Agent, Hardware Device, Role, and Task, each with a tailored enrollment flow and its own visual iconography [4]. Autonomous agents register their own UIID accounts through a machine-readable skill.md protocol that advertises operational capabilities and enables automated handshakes with other nodes. Static secrets and long-lived access keys are replaced with dynamic, single-use or multi-use

provisioning tokens issued from a centralized Agent Factory dashboard, from which the controlling human or organization can spin up new machine processes and monitor fleet activity, resource consumption, and trust scores in real time; intercepted tokens cannot be weaponized to compromise the broader autonomous fleet [4].

D. Device Decoupling

UIID is intentionally decoupled from the physical device on which it is used: biometric material for enrollment is stored locally on the WYNIX endpoint rather than on a remote server, and proofs to relying parties are produced as zero-knowledge attestations rather than by transmitting the underlying attributes. This decoupling is what allows the same UIID to be presented across the six higher layers without any of those layers gaining custody of the underlying key material.

E. Cryptographic Suite

The current UIID reference implementation uses Ed25519 for authentication and assertion signatures and X25519 for key agreement, consistent with common practice among deployed DID methods. The formal did:uiid method specification — analogous to the specifications collected in the W3C DID Specification Registries [5] — is under active preparation and will define supported verification-method types explicitly.

IV. VIVON — PHYSICAL WEB4 MOBILE ACCESS (L2)

VIVON is the LINKSPREED reference implementation of the L2 sovereign physical access layer specified in [1, Section IV-B]. It provides global eSIM connectivity independent of a single national mobile network operator, and exposes UIID-native primitives for voice and messaging so that a subject's did:uiid identifier can act as the addressable endpoint for a call or a chat message in the same way a phone number does under the E.164 numbering plan, without the number itself ever being issued or held by a telecommunications carrier.

VIVON is the layer at which the physical connection to the network is bound to the UIID identity substrate rather than to an operator-issued subscriber identifier. A subject retains reachability under their own did:uiid when moving between jurisdictions or carriers, and inbound voice and messaging traffic is delivered to the current active endpoint under the same DID regardless of the underlying physical carrier.

V. ARCTIC — DECENTRALIZED COMPUTE BACKBONE (L3)

A. Component Overview

ARCTIC is the LINKSPREED reference implementation of the L3 decentralized compute mesh specified in [1, Section IV-C]. It composes idle end-user hardware into an agentic-compute mesh in which state is synchronized under a Byzantine-fault-tolerant consensus scheme and persisted through a zero-knowledge storage layer (Zk-Storage Mesh) that shards ciphertext across participating nodes rather than concentrating it in a single operator's cluster.

B. ARCTIC OS

ARCTIC nodes present a common execution environment through ARCTIC OS, which exposes the UIID identity substrate at the operating-system level so that a call into a compute resource is authorized under the same DID and scope as a call into any other Web4 service. The architectural consequence is that compute is procured under the same sovereignty model as identity: the workload is bound to the UIID that authorized it and to the capability grant under which it runs, rather than to an account issued by the compute operator.

C. Synthetic Web Execution

ARCTIC is the layer at which the Synthetic Web (defined in [1, Section IV-H]) is executed in the LINKSPREED implementation. An autonomous agent acting under a UIID-derived, time-boxed capability grant consumes compute cycles on ARCTIC nodes and records its outputs on the same mesh, without needing an intermediate hyperscale-provider account. Both agent-to-tool interaction (via the Model Context Protocol [6]) and agent-to-agent interaction (via the Agent-to-Agent protocol [7]) are executed on ARCTIC under UIID-scoped capability grants.

VI. HELION — INTELLIGENT NETWORK ROUTING AND NAMING (L4)

A. Component Overview

HELION is the LINKSPREED reference implementation of the L4 intelligent routing and naming layer specified in [1, Section IV-D]. It provides two functions that are conventionally furnished by separate operators on the legacy internet: intelligent network routing between Web4 endpoints, and the Linkspreed Name Service (LNS) — a decentralized name service that replaces the ICANN/DNS hierarchy for names inside the Web4 stack.

B. Linkspreed Name Service (LNS)

Under LNS, a name is registered as a record whose controller is a did:uiid identifier, so ownership of the name is bound to sovereign identity rather than to a recurring registrar contract. LNS additionally serves the verifiable-data-registry role defined in W3C DID Core [3] for did:uiid resolution: DID Documents are resolved via LNS records, and Alias-Identifier verification anchors terminate on LNS. Consistency and update-propagation guarantees of LNS therefore directly bound the security properties of the deployed stack, as discussed in [1, Section V-B].

C. W4 OS, OXYGEN, and W4 Search

HELION additionally provides the W4 OS integration surface at which higher-layer applications (TRIVE, ATRIUM, WYNIX) resolve LNS records into ARCTIC endpoints. The OXYGEN browser is the Web4-native browser that resolves LNS-anchored URIs directly and performs UIID-scoped session establishment against reached endpoints. W4 Search is the corresponding discovery surface for LNS-anchored resources.

VII. TRIVE — UIID-AUTHENTICATED SAAS LAYER (L5)

A. Component Overview

TRIVE is the LINKSPREED reference implementation of the L5 DID-authenticated service layer specified in [1, Section IV-E]. It is the developer-facing SaaS layer of the stack, providing UIID-authenticated tooling that consumes the identity, routing, and compute layers below it without reimplementing them.

B. B2B and B2C Suites

TRIVE is organized into two suites: a business-to-business (B2B) suite oriented at enterprise deployments, and a business-to-consumer (B2C) suite of applications supported by a privacy-friendly, non-tracking advertising model. TRIVE applications do not maintain independent user databases; user state is written to the UIID key-value storage that is exposed to authenticated applications as an extension of the Core Identifier, so that a user's data associated with a TRIVE application remains addressable under the same DID after the application itself is retired or replaced.

VIII. ATRIUM — SUPER APPS AS A SERVICE (L6)

A. Component Overview

ATRIUM is the LINKSPREED reference implementation of the L6 sovereign application delivery layer specified in [1, Section IV-F]. It provides Super Applications as a Service (SNaaS): a customer can deploy a fully-featured social network or super-application on top of the underlying stack in under sixty seconds using LINKSPREED's 1-Prompt AI Method, in which the desired network is described in natural language and the corresponding ATRIUM configuration is generated and deployed against the lower layers.

B. Tenant Isolation and Credential Portability

ATRIUM instances are tenant-isolated so that operators can deploy independently branded, independently configured super-applications while still relying on the shared UIID identity substrate. A credential issued in one instance is portable to another without re-registration, because the underlying subject is anchored at L1 rather than at the tenant level.

C. Termination Point for Human and Synthetic Traffic

ATRIUM is the layer at which both human-session traffic and Synthetic-Web traffic terminate in the deployed LINKSPREED stack; it is therefore the layer at which the structural distinction between the two traffic classes, defined in [1, Section IV-H], becomes operationally visible.

IX. WYNIX — CERTIFIED CONSUMER HARDWARE (L7)

A. Component Overview

WYNIX is the LINKSPREED reference implementation of the L7 sovereign hardware layer specified in [1, Section IV-G]. Its two flagship components are the W4 Phone and the ARCTIC micro-server.

B. The W4 Phone

The W4 Phone is a smartphone that operates as a personal server: it hosts the user's ATRIUM tenant and UIID key material on-device rather than in a remote provider's cluster, and terminates VIVON connectivity on the same device. The consequence is that the same physical device holds L1 key material, terminates L2 connectivity, hosts the user's L6 tenant, and provides the biometric enrollment surface referred to in Section III-D above.

C. The ARCTIC Micro-Server

The ARCTIC micro-server is a low-power appliance intended to bring an ARCTIC node into the home so that a household's Web4 activity can execute locally rather than being routed to third-party infrastructure — the deployment pattern LINKSPREED refers to as Web4@Home.

D. Root of Trust

WYNIX is the layer at which the sovereignty guarantees asserted at Layers L1–L4 are physically realized on a device the user actually controls; where a deployment requires hardware-bound key custody, WYNIX is the layer at which that root of trust is provisioned.

X. END-TO-END REQUEST LIFECYCLE IN THE DEPLOYED STACK

A request path in the deployed LINKSPREED implementation proceeds as follows. A client device — typically a WYNIX endpoint reaching the network over a VIVON eSIM — issues a UIID-signed request to the receiving ATRIUM instance (step 1). ATRIUM dispatches the underlying intent through TRIVE, which resolves the target endpoint via the HELION Linkspreed Name Service and consults UIID for a scoped capability grant tied to the acting Alias Identifier (steps 2–4). The resulting action is executed against the ARCTIC compute mesh and anchored as an independently addressable artifact under HELION's LNS namespace (step 5), so that both pre-action authorization and post-action attribution are cryptographically anchored rather than log-based.

For Synthetic-Web traffic, the request originates not from a WYNIX endpoint under an interactive human session, but from an AI Agent registered in UIID (per Section III-C above) acting under a time-boxed capability grant issued by its controlling Human Individual or Organization principal. All subsequent steps are identical, except that ATRIUM and TRIVE distinguish traffic classes based on the grant metadata and can apply differentiated policy (e.g., rate limiting, scope restriction, human-in-the-loop confirmation) accordingly.

XI. RELEASE STATUS AND ROADMAP

At the time of publication, the components described above are at differing levels of release maturity. UIID is in production at v2.8, incorporating the multi-entity framework and Agent Factory features described in Section III-C [4]. VIVON, HELION, TRIVE, and ATRIUM are deployed and operating against production UIID. ARCTIC is in staged rollout, with the Zk-Storage Mesh in ongoing hardening. WYNIX is under active hardware development; the W4 Phone and the ARCTIC micro-server are the two flagship devices.

Concrete open items for the next release cycle include: (i) publication of the formal did:uiid method specification for entry in the W3C DID Specification Registries [5]; (ii) implementation and independent cryptographic audit of the BBS+ selective-disclosure scheme at the Alias Identifier verification point, on which the unlinkability property discussed in [1, Section V-B] depends; (iii) publication of an IETF Internet-Draft describing the Web4 capability grant format defined in [1, Section IV-H]; and (iv) hardware certification for the WYNIX flagship devices.

XII. CONCLUSION

This companion technical report has specified the concrete LINKSPREED reference implementation of the seven-layer sovereign-ownership architecture defined in [1]. The mapping from abstract layers L1–L7 to the seven named components

UIID, VIVON, ARCTIC, HELION, TRIVE, ATRIUM, and WYNIX has been given in Table I. Each component has been described in a dedicated section (III–IX), the end-to-end request lifecycle in the deployed stack has been described in Section X, and the current release status and near-term roadmap have been documented in Section XI.

Readers seeking the architectural justification of the seven-layer stack, the formal statement of the Ownership Thesis, the standards positioning, and the comparative security analysis are referred to the architectural specification [1]. Readers seeking to build against the deployed LINKSPREED implementation are referred to the developer resources at web4.one and uiid.linkspreed.com [8].

ACKNOWLEDGMENT

The author thanks the LINKSPREED GROUP Web4 Division and all engineering teams contributing to the UIID, VIVON, ARCTIC, HELION, TRIVE, ATRIUM, and WYNIX product surfaces.

REFERENCES

[1] M. Herdina, "Web4: A Seven-Layer Sovereign-Ownership Architecture for the Next Generation of the Internet — The Ownership Thesis, Layered Reference Architecture, and Security Analysis," LINKSPREED GROUP, 2026. (Architectural specification; companion paper to the present report.)

[2] W3C, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022. [Online]. Available: https://www.w3.org/TR/did-1.0/

[3] W3C, "Decentralized Identifiers (DIDs) v1.1," W3C Candidate Recommendation Snapshot, 5 Mar. 2026. [Online]. Available: https://www.w3.org/TR/2026/CR-did-1.1-20260305/

[4] M. Herdina, "UIID v2.8: Sovereign Machine Identity — Autonomous Agent Enrollment, Agent Factory, Zero-Trust Provisioning," Technical Announcement, LINKSPREED GROUP, Jun. 2026.

[5] W3C DID Working Group, "DID Specification Registries," W3C Group Note.

[6] Model Context Protocol Working Group, "Model Context Protocol Specification," 2024–2026. [Online]. Available: https://modelcontextprotocol.io/specification

[7] A2A Project, "Agent2Agent (A2A) Protocol Specification, v1.0.0," 2026. [Online]. Available: https://a2aprotocol.org/latest/specification/

[8] LINKSPREED GROUP, "Web4 — The Spatial Internet Infrastructure: UIID, VIVON, ARCTIC, HELION, TRIVE, ATRIUM, WYNIX," Architecture Overview. [Online]. Available: https://web4.one and https://uiid.linkspreed.com

[9] W3C, "Verifiable Credentials Data Model v2.0," W3C Recommendation. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/

[10] NIST Center for AI Standards and Innovation (CAISI), "AI Agent Standards Initiative," announcement, 17 Feb. 2026.